



日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 2 月 2 8 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 0 5 3 3 6 2
Application Number:

[ST. 10/C] : [J P 2 0 0 3 - 0 5 3 3 6 2]

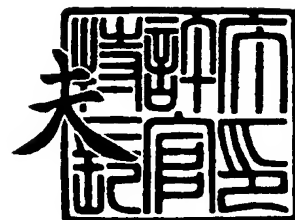
出 願 人 松 下 電 器 産 業 株 式 会 社
Applicant(s):



2 0 0 4 年 1 月 1 4 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康



出証番号 出証特 2 0 0 3 - 3 1 1 1 5 1 3



【書類名】 特許願

【整理番号】 2030750003

【提出日】 平成15年 2月28日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 G06F 15/00

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

 【氏名】 峰村 淳

【特許出願人】

 【識別番号】 000005821

 【氏名又は名称】 松下電器産業株式会社

【代理人】

 【識別番号】 100099254

 【弁理士】

 【氏名又は名称】 役 昌明

【選任した代理人】

 【識別番号】 100100918

 【弁理士】

 【氏名又は名称】 大橋 公治

【選任した代理人】

 【識別番号】 100105485

 【弁理士】

 【氏名又は名称】 平野 雅典

【選任した代理人】

 【識別番号】 100108729

 【弁理士】

 【氏名又は名称】 林 紘樹

**【手数料の表示】****【予納台帳番号】** 037419**【納付金額】** 21,000円**【提出物件の目録】****【物件名】** 明細書 1**【物件名】** 図面 1**【物件名】** 要約書 1**【包括委任状番号】** 9102150**【包括委任状番号】** 9116348**【包括委任状番号】** 9600935**【包括委任状番号】** 9700485**【プルーフの要否】** 要

【書類名】 明細書

【発明の名称】 アプリケーション認証システムと装置

【特許請求の範囲】

【請求項 1】 安全な情報秘匿領域を持たない端末に固定的にまたは着脱可能に接続されたセキュアデバイスが、前記端末に格納されたアプリケーションを認証するアプリケーション認証システムであって、

セキュアデバイスは、端末上のアプリケーション実行手段を認証し、前記アプリケーション実行手段の、セキュアデバイスへのアクセスを要求するアプリケーションに関する処理に基づいて、前記アプリケーションを認証することを特徴とするアプリケーション認証システム。

【請求項 2】 前記アプリケーション実行手段は、電子署名が付された前記アプリケーションのダイジェストデータを算出して、前記ダイジェストデータと前記電子署名とをセキュアデバイスに提示し、セキュアデバイスは、提示されたダイジェストデータを用いて前記電子署名を検証し、検証結果が正常であるとき、前記アプリケーションを認証することを特徴とする請求項 1 に記載のアプリケーション認証システム。

【請求項 3】 前記アプリケーション実行手段は、前記アプリケーションのダイジェストデータを算出して、前記ダイジェストデータをセキュアデバイスに提示し、セキュアデバイスは、提示されたダイジェストデータを自ら保持するダイジェストデータと照合し、照合結果が正常であるとき、前記アプリケーションを認証することを特徴とする請求項 1 に記載のアプリケーション認証システム。

【請求項 4】 前記アプリケーション実行手段は、前記アプリケーションのダイジェストデータを算出した後、セキュアデバイスに対して処理要求命令を送出し、セキュアデバイスは、第一の情報をアプリケーション実行手段へ送出し、アプリケーション実行手段は、前記第一の情報を前記ダイジェストデータで暗号化してセキュアデバイスに送出し、セキュアデバイスは、前記暗号化された情報を自ら保持するダイジェストデータで復号し、復号によって得られる情報と前記第一の情報とを照合することを特徴とする請求項 3 に記載のアプリケーション認証システム。

【請求項 5】 前記アプリケーション実行手段は、電子署名が付された前記アプリケーションの前記電子署名を検証して前記アプリケーションを認証し、セキュアデバイスは、前記アプリケーション実行手段の認証結果を受け入れて前記アプリケーションを認証することを特徴とする請求項 1 に記載のアプリケーション認証システム。

【請求項 6】 セキュアデバイスが前記アプリケーション実行手段を認証した際に、セキュアデバイスと前記アプリケーション実行手段とで第二の情報を共有し、セキュアデバイスは、セキュアデバイスが認証したアプリケーションからの処理要求に前記第二の情報が加味されている場合に、その処理要求を受け付けることを特徴とする請求項 2 から 5 のいずれかに記載のアプリケーション認証システム。

【請求項 7】 端末に固定的にまたは着脱可能に接続されたデバイスであって、前記端末を認証する処理を行うカードマネージャと、前記端末に格納された、アクセスを要求するアプリケーションに対して認証処理を行うカードアプリケーションとを備え、前記カードアプリケーションは、前記端末が前記アプリケーションに対して行った処理に基づいて前記アプリケーションを認証し、前記カードマネージャの前記端末を認証する処理が完了していることを確認して、認証した前記アプリケーションのアクセス要求を受け付けることを特徴とするセキュアデバイス。

【請求項 8】 アプリケーション実行手段と、アプリケーションとを備え、前記アプリケーション実行手段は、装着されたセキュアデバイスが前記アプリケーション実行手段を認証した後、セキュアデバイスへのアクセスを要求する前記アプリケーションのダイジェストデータを算出し、前記ダイジェストデータを用いて前記アプリケーションを認証した後、前記セキュアデバイスにアクセス要求を行うことを特徴とする端末。

【請求項 9】 前記アプリケーション実行手段は、前記ダイジェストデータを用いて前記アプリケーションに付された電子署名を検証し、前記アプリケーションを認証することを特徴とする請求項 8 に記載の端末。

【請求項 1 0】 前記アプリケーション実行手段は、前記ダイジェストデー

タを前記セキュアデバイスに送り、前記セキュアデバイスから前記ダイジェストデータの照合結果を取得して、前記アプリケーションを認証することを特徴とする請求項 8 に記載の端末。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ＩＣカードなどのセキュアデバイス上で動作するカードアプリケーションが、携帯端末などの端末上で動作するアプリケーションを認証するアプリケーション認証システムと、そのセキュアデバイスと端末に関し、特に、端末上のアプリケーションがセキュアデバイスを利用する際に必要となる認証処理を実現するものである。

【0002】

【従来の技術】

近年、情報をセキュアに格納することが可能なＩＣカードなどのセキュアデバイスは、電子商取引や入退出管理、定期券など、多方面で利用されており、今後、携帯端末などのモバイル機能を活用して、その利用範囲は、益々広がるものと見られている。

【0003】

図 8 には、携帯端末 30 上で動作するアプリケーション（以下、省略して「アプリ」と言う）が、セキュアデバイス 10 に格納されたセキュアなデータを利用して実行可能となると見られているサービスの数々を模式的に示している。

セキュアデバイス内で動作するアプリ（カードアプリ）は、下記非特許文献 1 に記載されているように、Java(登録商標)などのプログラミング言語で作成されてセキュアデバイスに搭載される。カードアプリは、セキュアデバイスに格納したセキュアなデータの利用を求める外部アプリに対して、認証を行い、安全性を確認してから、外部アプリのコマンドを受け付ける。

【0004】

【非特許文献 1】

「Interface」2003 年 3 月号、CQ 出版社、p. 82～90

【0 0 0 5】

【発明が解決しようとする課題】

しかし、従来のセキュアデバイスは、携帯端末にダウンロードされたアプリに対する認証手段を有しておらず、そのため、携帯端末にダウンロードされたアプリは、セキュアデバイスに格納されたデータを利用することができない。

これは、次のような事情に拠る。

通常、認証処理では、本人しか知り得ない情報を知っているかどうかを確認し、知っている場合に、本人と認める。図 9 は、この方式による相互認証をセキュアデバイス 1 0 のカードアプリ 1 1 と、携帯端末 3 0 の端末アプリ（ここでは Java(登録商標) 言語で記述された Java(登録商標) アプリとする） 3 1 とに当て嵌めたときの様子を模式的に示している。機密データの保管機能を持つセキュアデバイス 1 0 は、ハードウェア的に安全に作られた耐タンパ性の領域に秘密の情報（暗号鍵など）を保持することができる。一方、携帯端末 3 0 が秘密情報を扱うには、セキュリティが要求されるため、領域 3 1 全体が耐タンパ性であるか、秘密情報を保持する耐タンパ性の領域 3 5 が在って、領域 3 1 が領域 3 5 に認証されている必要がある。こうした状況にあれば、カードアプリ 1 1 と、携帯端末 3 0 の OS（あるいは VM（virtual machine）） 3 2 の制御の下で動作する Java(登録商標) アプリ 3 1 とが情報を交換し、互いに共通の秘密情報を保持していることが確認できれば、相互認証は成立する。

【0 0 0 6】

しかし、実際には、携帯端末 3 0 は、秘密情報を安全に保持できる領域を有していない。そのため、カードアプリ 1 1 は、共通の秘密情報を用いて相手認証を行うことができず、従って、携帯端末 3 0 にダウンロードされた Java(登録商標) アプリ 3 1 は、これまで、セキュアデバイス 1 0 に格納されたデータを利用することができなかった。

こうした事情から、携帯端末 3 0 にセキュアデバイス 1 0 を装着して、ネットワークを通じてサービスサーバからサービスを受ける場合でも、これまでは、セキュアデバイス 1 0 と相互認証したサービスサーバは、セキュアデバイス 1 0 に格納されたデータを利用できるが、携帯端末 3 0 は、データをスルーする土管の

役割しか果たすことができなかった。そのため、図 8 に示すように、携帯端末 30 のアプリがセキュアデバイス 10 のデータを読み／書きして、計算や表示などの高度の処理を行うシステムは実現することができなかった。

【0007】

本発明は、こうした従来の問題点を解決するものであり、安全な情報秘匿領域を持たない端末上のアプリに対するセキュアデバイスの認証が可能なアプリケーション認証システムを提供し、そのシステムを構成するセキュアデバイス及び端末を提供することを目的としている。

【0008】

【課題を解決するための手段】

そこで、本発明では、安全な情報秘匿領域を持たない端末に固定的にまたは着脱可能に接続されたセキュアデバイスが、前記端末に格納されたアプリを認証するアプリケーション認証システムにおいて、セキュアデバイスが、端末上のアプリ実行手段を認証し、このアプリ実行手段の、セキュアデバイスへのアクセスを要求するアプリに関する処理に基づいて、アプリを認証するように構成している。

【0009】

また、本発明では、端末に固定的にまたは着脱可能に接続されるセキュアデバイスに、端末を認証する処理を行うカードマネージャと、端末に格納された、アクセスを要求するアプリに対して認証処理を行うカードアプリケーションとを設け、カードアプリケーションは、端末がアプリに対して行った処理に基づいてアプリを認証し、カードマネージャの前記端末を認証する処理が完了していることを確認して、認証したアプリのアクセス要求を受け付けるように構成している。

【0010】

また、本発明では、アプリ実行手段と、アプリとを備える端末において、アプリ実行手段は、装着されたセキュアデバイスがアプリ実行手段を認証する処理の完了後、セキュアデバイスへのアクセスを要求するアプリのダイジェストデータを算出し、このダイジェストデータを用いてアプリを認証した後、セキュアデバイスにアクセス要求を行うように構成している。

【 0 0 1 1 】

そのため、セキュアデバイスの端末認証、及び、端末内でのアプリの認証とを結び付けることで、安全な情報秘匿領域を持たない端末上で動作するアプリに対して、セキュアデバイスによる認証が可能になる。

【 0 0 1 2 】**【発明の実施の形態】****（第 1 の実施形態）**

本発明の第 1 の実施形態におけるアプリケーション認証システムでは、携帯端末上で動作する端末アプリを認証するため、セキュアデバイスのカードアプリは、端末アプリが正規のアプリであるか否かを確認する。カードアプリは、端末アプリが正規のアプリと確認できたとき、認証処理が正常に終了したものとして、端末アプリのアクセス要求を受け付ける。

【 0 0 1 3 】

図 2 は、このシステムを構成するセキュアデバイス 1 0 と携帯端末 3 0 とを模式的に示している。携帯端末 3 0 は、工場出荷時に情報が R O M やフラッシュメモリに書き込まれ、以後、情報の書き換えができない「書き換え不可領域 3 0 2」と、ダウンロードされたアプリが書き込まれる「ユーザ書き換え領域 3 0 1」とを備えており、ユーザ書き換え領域 3 0 1 には、電子署名 3 4 が付された Java (登録商標) アプリ 3 1 が格納され、また、書き換え不可領域 3 0 2 には、O S 3 2 や、Java (登録商標) 言語で記述されたプログラムを実行するための Java (登録商標) 実行環境 (J A M) 3 3 が格納されている。

【 0 0 1 4 】

なお、「書き換え不可領域 3 0 2」は、端末上の操作（例えば、アプリケーション 3 1）や、外部（例えば、カード 1 0）からのアクセスなどにより、そこに格納された情報が書き換えられないことがない領域を意味し、その領域自身が物理的書き換え不可能な仕組み（例えば R O M）を有しているか否かは問わない。

【 0 0 1 5 】

Java (登録商標) アプリ 3 1 の電子署名 3 4 は、Java (登録商標) アプリ 3 1 の正当性を証明する認証局によって付されており、Java (登録商標) アプリ 3 1 のデー

タにハッシュ演算を行ってダイジェストデータを生成し、このダイジェストデータを認証局の秘密鍵で暗号化して生成されている。

また、JAM33には、携帯端末30がセキュアデバイス10との相互認証に用いる端末認証情報と、電子署名34の検証用公開鍵を含む認証局のアプリ証明書とが入力される（ここで「入力される」とは、それぞれの情報が、コードとしてJAM33に埋め込まれたり、必要なときにファイルとして取得可能であることを意味する）。

【0016】

一方、セキュアデバイス10は、携帯端末30に対する認証処理を行う共通ライブラリ（カードマネージャ）13と、携帯端末30で動作するJava（登録商標）アプリ31の認証処理を行うカードアプリ11と、認証局の公開鍵を証明する署名検証用ルート証明書14とを備えている。

【0017】

また、カードマネージャ13には、セキュアデバイス10が携帯端末30との相互認証に用いる端末認証情報が入力される（ここで「入力される」とは、それぞれの情報が、コードとしてカードマネージャ13に埋め込まれたり、必要なときにファイルとして取得可能であることを意味する）。

【0018】

なお、本発明では、セキュアデバイス10が携帯端末30を認証することは必要であるが、携帯端末30がセキュアデバイス10を認証することは必ずしも必要ではない。各実施形態では、セキュアデバイス10と携帯端末30とが「相互認証」する場合について示しているが、相互認証は必須ではなく、セキュアデバイス10が携帯端末30を認証する「片側認証」で良い。

【0019】

図1には、このシステムにおいて、セキュアデバイス10のカードアプリ11が、携帯端末30で動作するJava（登録商標）アプリ31を認証するまでの手順を矢印で示している。

セキュアデバイス10が携帯端末30に装着されると、セキュアデバイス10のカードマネージャ13は、携帯端末30のJAM33との間で、それぞれの端

末認証情報を用いて、装置間の相互認証処理を行う（1）。相互認証に成功すると、カードマネージャ 1 3 は、その成功を示すフラグ（相互認証パスフラグ）をセキュアデバイス 1 0 内に立てる。

【0 0 2 0】

なお、セキュアデバイスによる端末の認証方式については、種々のものが知られており、このシステムでも、それらの方式を用いることができる。例えば、T C P A（Trusted Computing Platform Alliance）の方式を用いて、セキュアデバイスが B I O S（Basic Input Output System）を認証後、B I O S が O S を認証し、次に、O S が Java（登録商標）実行環境を認証するようにしてもよい。また、耐タンパ性の S I M カードやセキュア L S I を持つ携帯端末の場合には、チャレンジ&レスポンス（challenge&response）方式を用いることができる。要は、正規端末であることの認証が出来れば良く、特定機器へのバインド方式であっても一向構わない。

【0 0 2 1】

携帯端末 3 0 の J A M 3 3 は、セキュアデバイス 1 0 との相互認証に成功すると、セキュアデバイス 1 0 へのアクセス機能を開始し、Java（登録商標）アプリ 3 1 は、J A M 3 3 に対してセキュアデバイス 1 0 へのアクセスを要求する（2-1）。この要求を受けた J A M 3 3 は、アプリ証明書に含まれる公開鍵を用いて Java（登録商標）アプリ 3 1 の電子署名 3 4 を検証し、それにより Java（登録商標）アプリ 3 1 を認証する（2-2）。

【0 0 2 2】

電子署名 3 4 の検証は、Java（登録商標）アプリ 3 1 のデータにハッシュ演算を行ってダイジェストデータを生成し、このダイジェストデータと、電子署名 3 4 を公開鍵で復号化したデータとを比較することによって行われる。それらが一致する場合には、J A M 3 3 は、Java（登録商標）アプリ 3 1 の正当性を認証し、データが改ざんされていないことを確認することができる。

【0 0 2 3】

Java（登録商標）アプリ 3 1 を認証した J A M 3 3 は、生成したダイジェストデータと、Java（登録商標）アプリ 3 1 の電子署名 3 4 とをセキュアデバイス 1 0 の

カードアプリ 1 1 に提示する（2 - 3）。これを受けて、カードアプリ 1 1 は、署名検証用ルート証明書 1 4 から得た公開鍵を用いて電子署名 3 4 を復号化し、J A M 3 3 から送られたダイジェストデータとの一致を検証する。

Java(登録商標)アプリ 3 1 を認証した J A M 3 3 は、Java(登録商標)アプリ 3 1 からのアクセス要求を実行し、カードアプリ 1 1 にコマンドを送信する（3）。ダイジェストデータの検証に成功したカードアプリ 1 1 は、カードマネージャ 1 3 による機器認証が完了していることを相互認証パスフラグで確認した後、このコマンドを受け付ける。

【 0 0 2 4 】

このように、このアプリケーション認証システムのセキュアデバイスは、携帯端末で動作するアプリが正規のものであることを確認することで、そのアプリを認証する。そして、この確認を行うため、第 1 段階では、携帯端末を認証することにより、携帯端末の書き換え不可領域に格納されたJava(登録商標)実行環境（アプリ実行手段）の正当性を確認する。この確認が一度得られれば、アプリ実行手段の書き換えは不可能であるため、アプリ実行手段に対する信頼性は、その後も継続することとなる。

【 0 0 2 5 】

第 2 段階では、携帯端末の中でセキュアデバイスの信頼性を得たアプリ実行手段が、電子署名付きのアプリを認証し、このアプリのダイジェストデータと電子署名とをセキュアデバイスに渡す。

セキュアデバイスは、信頼を置くアプリ実行手段から、生成直後に渡されたダイジェストデータを信頼に足るものと見て、第 3 段階では、このダイジェストデータを電子署名によって検証する。

【 0 0 2 6 】

この検証結果が正常である場合、セキュアデバイスは、第 1 段階、第 2 段階、及び、第 3 段階の認証処理に基づいて、端末で動作するアプリが正規のアプリであると確認することができる。

このように、このアプリケーション認証システムでは、第 1 段階、第 2 段階、及び、第 3 段階の認証処理の連鎖により、セキュアデバイスが、安全な情報秘匿

領域を持たない端末上のアプリに対して認証することを可能にしている。

【0027】

(第2の実施形態)

本発明の第2の実施形態では、アプリを特定するための認証情報が格納されて発行されるセキュアデバイスと、そのアプリが動作する携帯端末とから成るアプリケーション認証システムについて説明する。

このセキュアデバイスは、携帯端末にダウンロードされるアプリと組になってサービスを実現するために作成されており、例えば、図8に示す「電子チケットアプリ」が携帯端末30にダウンロードされる場合では、セキュアデバイス10は、電子チケット用のセキュアデバイスと言うことになる。

【0028】

図4は、このシステムを構成するセキュアデバイス10と携帯端末30とを模式的に示している。携帯端末30のユーザ書き換え領域301に格納されているJava(登録商標)アプリ31は、署名を有していない。そのため、JAM33へのアプリ証明書の入力はない。また、セキュアデバイス10には、Java(登録商標)アプリ31を特定するためのダイジェストデータ15などのアプリ認証情報が予め格納されている。その他の構成は、第1の実施形態と変わりが無い。

【0029】

図3には、このシステムにおける認証手順を矢印で示している。

セキュアデバイス10が携帯端末30に装着されると、第1の実施形態(図1)と同様に、セキュアデバイス10のカードマネージャ13と、携帯端末30のJAM33との間で、装置間の相互認証処理が行われ(1)、相互認証に成功すると、カードマネージャ13は、その成功を示す相互認証パスフラグをセキュアデバイス10内に立てる。また、携帯端末30のJAM33は、セキュアデバイス10との相互認証に成功すると、セキュアデバイス10へのアクセス機能を開始し、Java(登録商標)アプリ31は、JAM33に対してセキュアデバイス10へのアクセスを要求する(2-1)。

【0030】

この要求を受けたJAM33は、Java(登録商標)アプリ31のデータにハッシ

ュ演算を行ってダイジェストデータを生成し（2-2）、このダイジェストデータをセキュアデバイス 10 のカードアプリ 11 に提示する（2-3）。カードアプリ 11 は、相互認証パスフラグを参照して、カードマネージャ 13 による機器認証が完了していることを確認した後、JAM 33 から提示されたダイジェストデータと、セキュアデバイス 10 内で密かに保持されているダイジェストデータ 15 とを照合し、認証結果を JAM 33 に返す（2-4）。Java(登録商標)アプリ 31 が認証されたことを知った JAM 33 は、Java(登録商標)アプリ 31 からのアクセス要求を実行し、カードアプリ 11 にコマンドを送信する（3）。

【0031】

このように、このアプリケーション認証システムでは、アプリに対する電子署名が不要（勿論、有っても構わない）であり、システムを簡略化できる。

また、オペレータがアプリに署名を付けるシステムでは、オペレータによる統制を排除できないが、アプリに対する電子署名が不要なこのシステムでは、オペレータの影響を受けずにビジネスを展開することができ、アプリのダウンロードが可能な体制を整えた上で、アプリの認証情報を埋め込んだセキュアデバイスをユーザに配布すれば、直ぐにサービスを開始することができる。

【0032】

なお、アプリ実行手段からセキュアデバイスへのアプリケーション認証のためのデータ（ダイジェストデータ）の提示処理である処理（2-3）のより具体的な方法としては、次のようなものが考えられる。例えば、PIN の照合などを行うときに使用する既存のコマンドの Verify を使用して、PIN の代わりにアプリ認証用のデータを提示する手法や、IC カードの外部認証で使用する challenge&responce 方式用の既存のコマンドである GetChallenge と ExternalAuthenticate において、秘密鍵の代わりにアプリ認証用のデータを使用して、データを提示する手法などである。

【0033】

後者の場合、通常の challenge-response 方式では、機器 B が機器 A を認証する場合、機器 A から機器 B に対して challenge-response 処理のトリガにあたる GetChallenge を送信すると、機器 B にて、あらかじめ保持されている情報や任意に

生成される情報（乱数など）である第一の情報を機器Aに返信して、機器Aにて前記第一の情報をあらかじめ保持している秘密鍵（秘密情報A）などで暗号化した上で機器Aに送信し（ExternalAuthenticate）、機器Bにて暗号化された情報をあらかじめ保持している秘密鍵（秘密情報B：秘密情報Aに対応した秘密情報）にて復号をし、復号によって得られる情報が、前記第一の情報と適合しているかを判断することになる。これを本発明に応用した場合、機器Aはアプリ実行手段33に、また、機器Bがカードアプリ11に相当するが、機器Aは秘密情報Aに相当するデータをセキュアに保持しておく領域を有しないため、秘密情報Aに替えてアプリ実行手段33が生成したダイジェストデータを、また、秘密情報Bに替えてセキュアデバイスがあらかじめ保持しているダイジェストデータ15をそれぞれ用いることで可能となる。

【0034】

（第3の実施形態）

本発明の第3の実施形態では、携帯端末の中でセキュアデバイスの信頼性を得たアプリ実行手段が、電子署名付きのアプリを認証し、この認証結果をセキュアデバイスが受け入れるアプリケーション認証システムについて説明する。

図6は、このシステムを構成するセキュアデバイス10と携帯端末30とを模式的に示している。セキュアデバイス10は、署名検証用ルート証明書を有していない。その他の構成は、第1の実施形態と変わりが無い。

【0035】

図5には、このシステムにおける認証手順を矢印で示している。

セキュアデバイス10が携帯端末30に装着されると、第1の実施形態（図1）と同様に、セキュアデバイス10のカードマネージャ13と、携帯端末30のJAM33との間で、装置間の相互認証処理が行われ（1）、相互認証に成功すると、カードマネージャ13は、その成功を示す相互認証パスフラグをセキュアデバイス10内に立てる。また、携帯端末30のJAM33は、セキュアデバイス10との相互認証に成功すると、セキュアデバイス10へのアクセス機能を開始し、Java（登録商標）アプリ31は、JAM33に対してセキュアデバイス10へのアクセスを要求する（2-1）。この要求を受けたJAM33は、アプリ証

明書に含まれる公開鍵を用いてJava(登録商標)アプリ 3 1 の電子署名 3 4 を検証し、それによりJava(登録商標)アプリ 3 1 を認証する (2-2)。この J A M 3 3 によるJava(登録商標)アプリ 3 1 の認証処理は、第 1 の実施形態で説明したものと同一である。

【0 0 3 6】

Java(登録商標)アプリ 3 1 を認証した J A M 3 3 は、Java(登録商標)アプリ 3 1 からのアクセス要求を実行し、カードアプリ 1 1 にコマンドを送信する (3)。セキュアデバイス 1 0 のカードアプリ 1 1 は、カードマネージャ 1 3 による機器認証が完了していることを相互認証パスフラグで確認した後、このコマンドを受け付ける。

このように、このアプリケーション認証システムのセキュアデバイスは、携帯端末との相互認証で、携帯端末の書き換え不可領域に格納されたJava(登録商標)実行環境 (アプリ実行手段) を認証すると、このアプリ実行手段により行われた、電子署名付きアプリの認証結果を信用して、このアプリを認証する。

【0 0 3 7】

このアプリケーション認証システムでは、アプリに署名を付ける方式を規定している既存方式 (J 2 S E など) がそのまま利用可能であり、また、こうした方式を用いてアプリへ署名を付けているシステムは、この実施形態のシステムに、障害無く移行することができる。

また、このシステムでは、第 2 の実施形態の場合とは逆に、アプリへの署名付けの権利を持つオペレータなどの主体は、ビジネスをコントロールすることができる。

【0 0 3 8】

なお、セキュアデバイスには、各実施形態で示したように、格納されているデータへのアクセスをカードアプリが制御するプログラムアプリ型のデバイスと、格納したファイルにアクセスするためのセキュリティ条件を決めるファイルアプリ型のデバイスとがある。後者のセキュアデバイスでは、図 7 に示すように、Java(登録商標)実行環境がカードマネージャの認証をパスした場合に、Java(登録商標)実行環境が選択する D F (Dedicated File) の傘下の E F (Elementary Fi

le) へのアクセスが可能になり、また、各実施形態の方式でアプリが認証された場合に、そのアプリが選択する D F の傘下の E F へのアクセスが可能になるようにセキュリティ条件を設定することができる。

【 0 0 3 9 】

なお、セキュアデバイスがアプリ実行手段を認証した後でも、セキュアデバイスにおける端末への装着部にある端子から、悪意のある人間によって、アプリ実行手段になりすましてあたかもアプリ実行手段からの信号であるかのようにセキュアデバイスに指示を送ることも不可能とは言い切れなく、そのような場合、このなりすましを防ぐためには、確かにアプリ実行手段からの指示であることを確認できる工夫があると更に好ましい。その工夫としては次のようなものが考えられる。

【 0 0 4 0 】

つまり、カードマネージャ 1 3 がアプリ実行手段 3 3 を認証する処理 (1) にて、カードマネージャ 1 3 からアプリ実行手段 3 3 へ任意の情報を送信して両方で共有するか、両者に共通の情報が保持されている (あるいは生成する) 場合はその情報を記憶しておく。この情報を第二の情報とすると、アプリ実行手段 3 3 からカードアプリ 1 1 へアクセス要求を行う処理 (3) にて、前記第二の情報も加味する。カードアプリ 1 1 では、受信したアクセス要求に第二の情報が加味されている要求のみを受付、加味されていなければなりすましなど不正なアクセスとみなしその処理を受け付けない。なお、ここで「第二の情報を加味」とは、アクセス要求に第二の情報を付加したり、アクセス要求の全部または一部の情報を、そのまま乃至加工したものを暗号化したりすることなどを意味する。

【 0 0 4 1 】

【発明の効果】

以上の説明から明らかなように、本発明のアプリケーション認証システムでは、安全な情報秘匿領域を持たない端末上で動作するアプリに対して、セキュアデバイスによる認証が可能になる。そのため、端末上のアプリは、端末に装着されたセキュアデバイスのデータへのアクセスが可能になり、高度な処理を実行することができる。

【図面の簡単な説明】**【図 1】**

本発明の第 1 の実施形態におけるアプリケーション認証システムの手順を示す

図

【図 2】

本発明の第 1 の実施形態におけるアプリケーション認証システムの構成を示す

図

【図 3】

本発明の第 2 の実施形態におけるアプリケーション認証システムの手順を示す

図

【図 4】

本発明の第 2 の実施形態におけるアプリケーション認証システムの構成を示す

図

【図 5】

本発明の第 3 の実施形態におけるアプリケーション認証システムの手順を示す

図

【図 6】

本発明の第 3 の実施形態におけるアプリケーション認証システムの構成を示す

図

【図 7】

本発明の実施形態におけるファイルアプリ型セキュアデバイスでのファイルアクセスを示す図

【図 8】

セキュアデバイスを装着した携帯端末で実現可能なサービスを示す図

【図 9】

携帯端末上のアプリをセキュアデバイスが認証するときの問題点を示す図

【符号の説明】

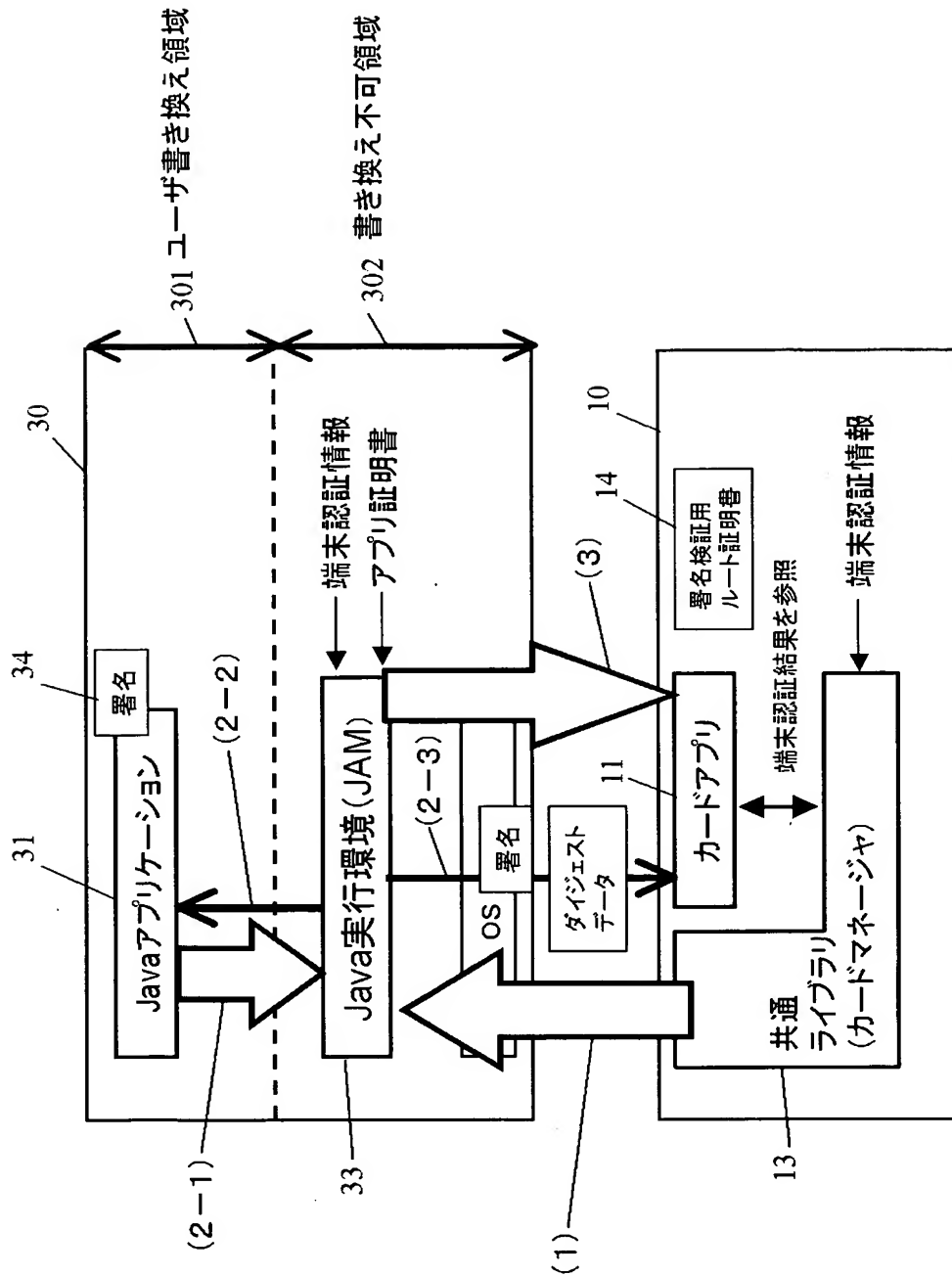
1 0 セキュアデバイス

1 1 カードアプリ

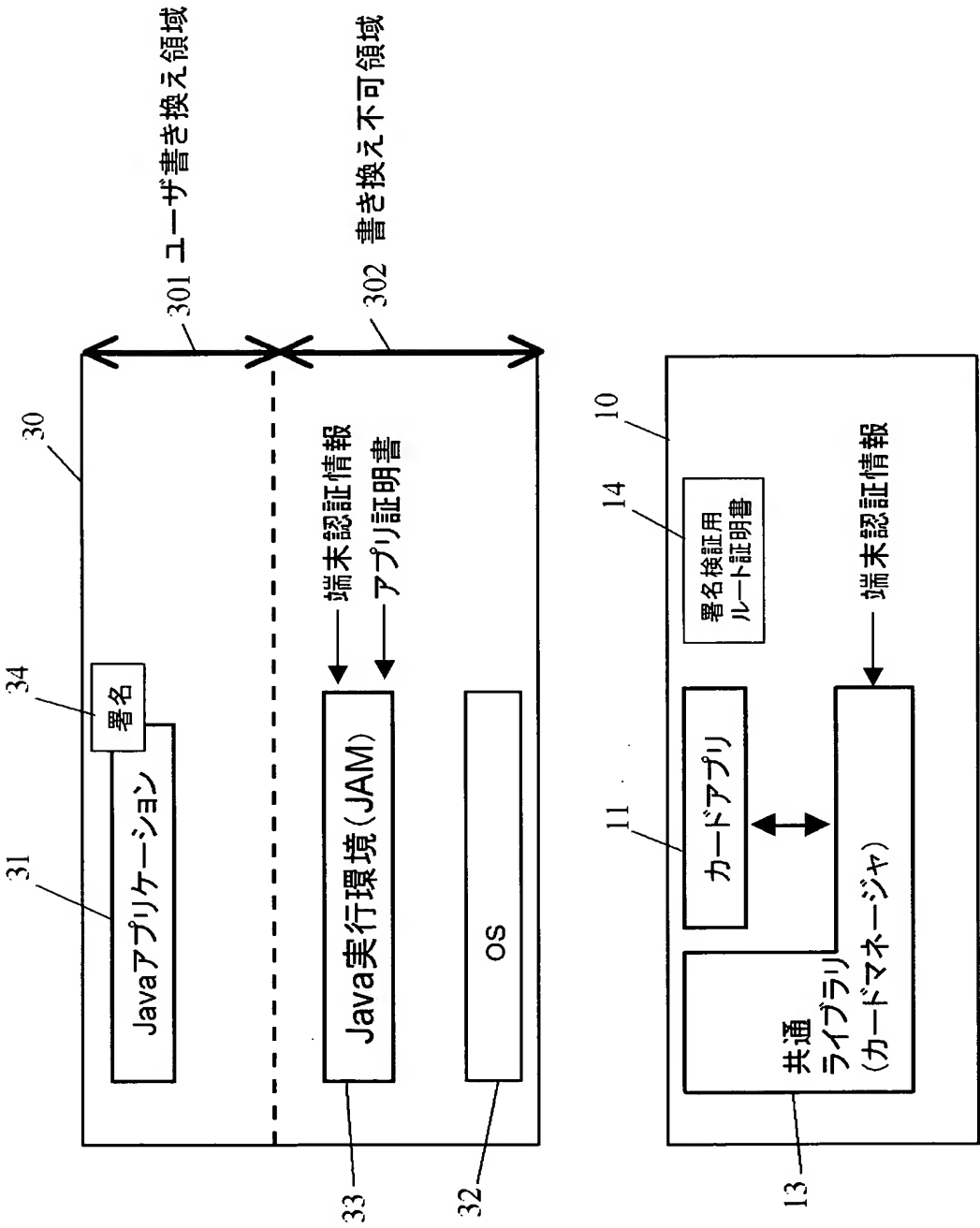
- 1 3 共通ライブラリ (カードマネージャ)
- 1 4 署名検証用ルート証明書
- 1 5 ダイジェストデータ
- 3 0 携帯端末
- 3 1 Java(登録商標) アプリ
- 3 2 O S
- 3 3 Java(登録商標) 実行環境 (J A M)
- 3 4 電子署名
- 3 5 秘密情報格納領域
- 3 0 1 ユーザ書き換え領域
- 3 0 2 書き換え不可領域

【書類名】 図面

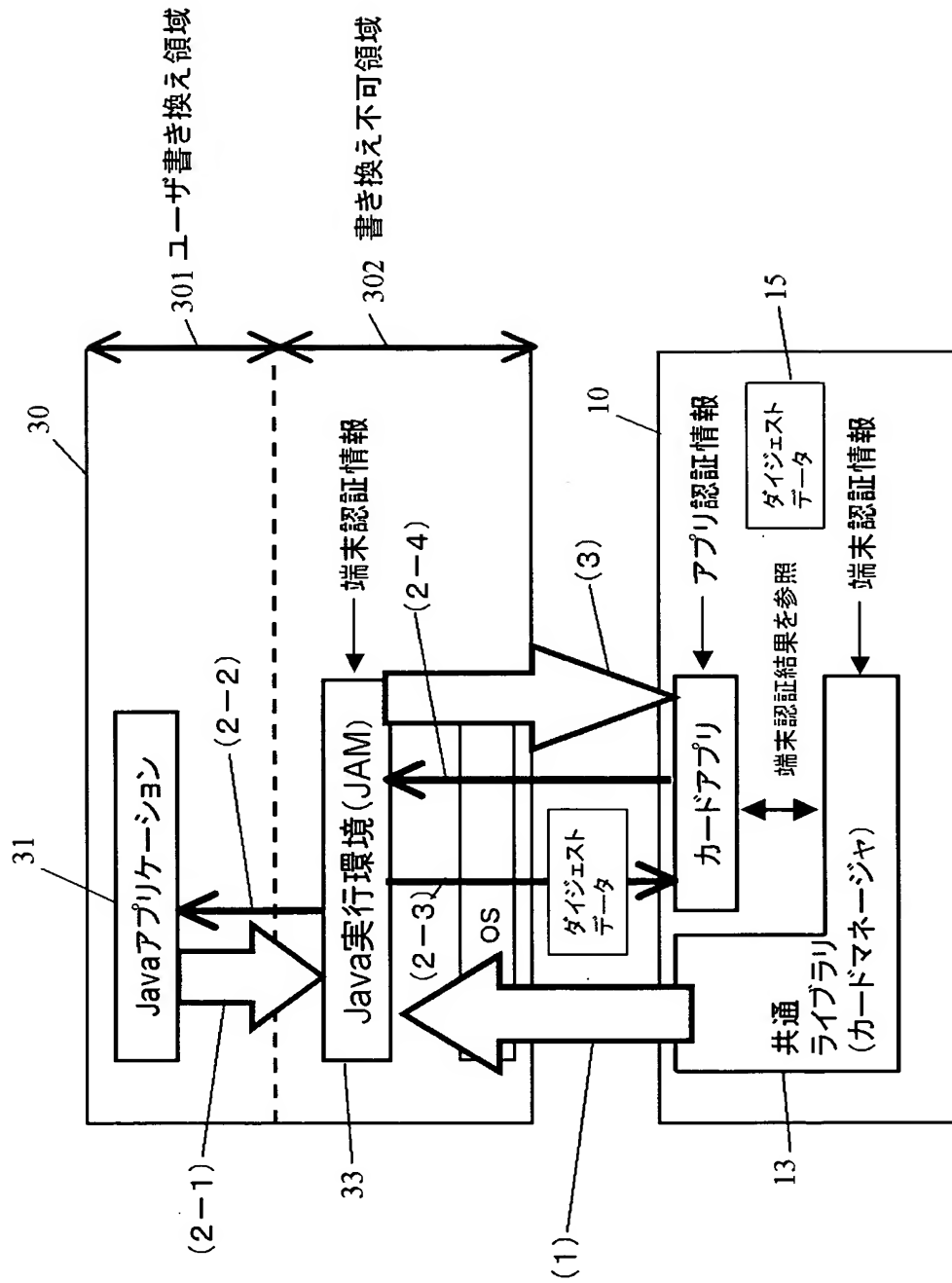
【図 1】



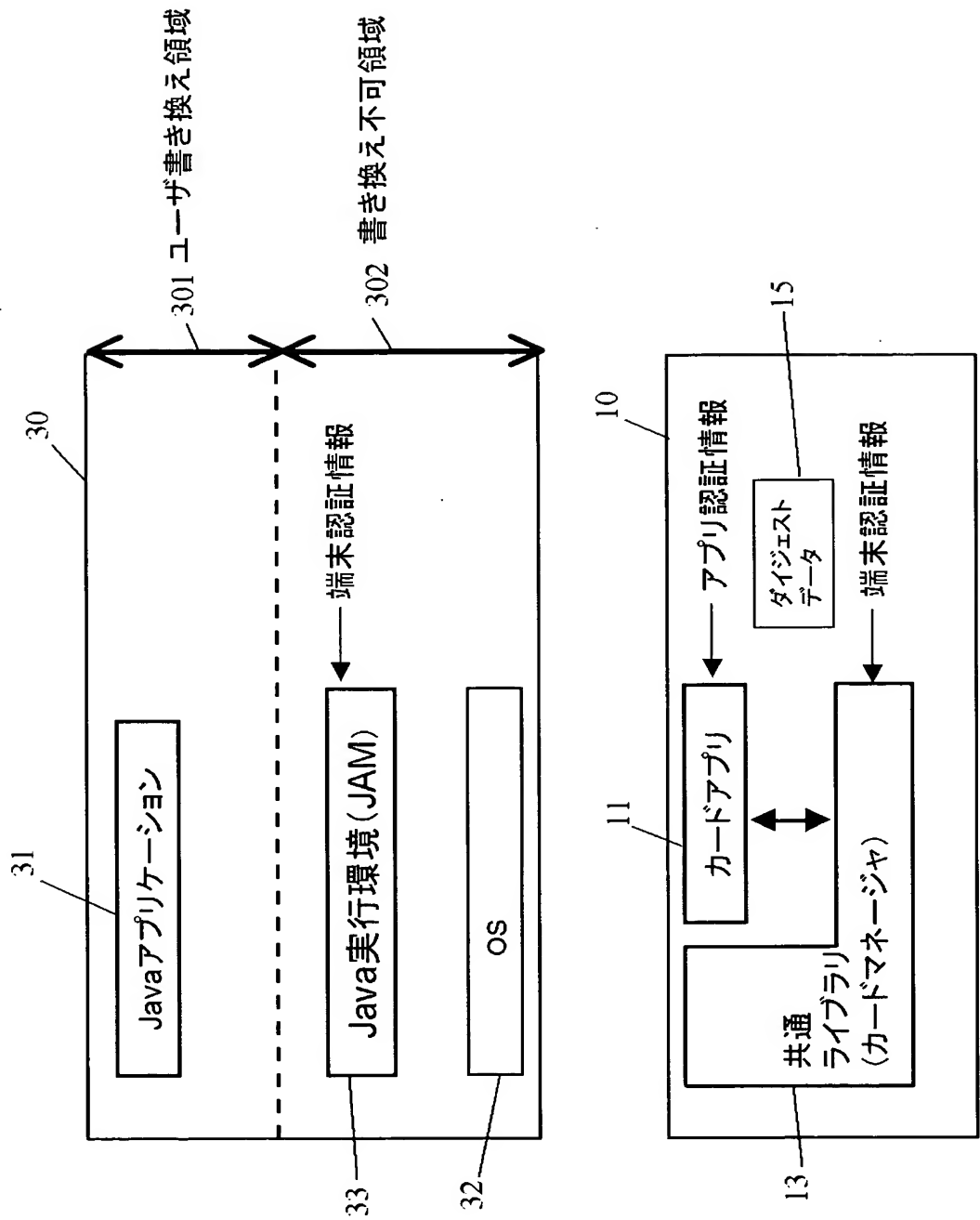
【図 2】



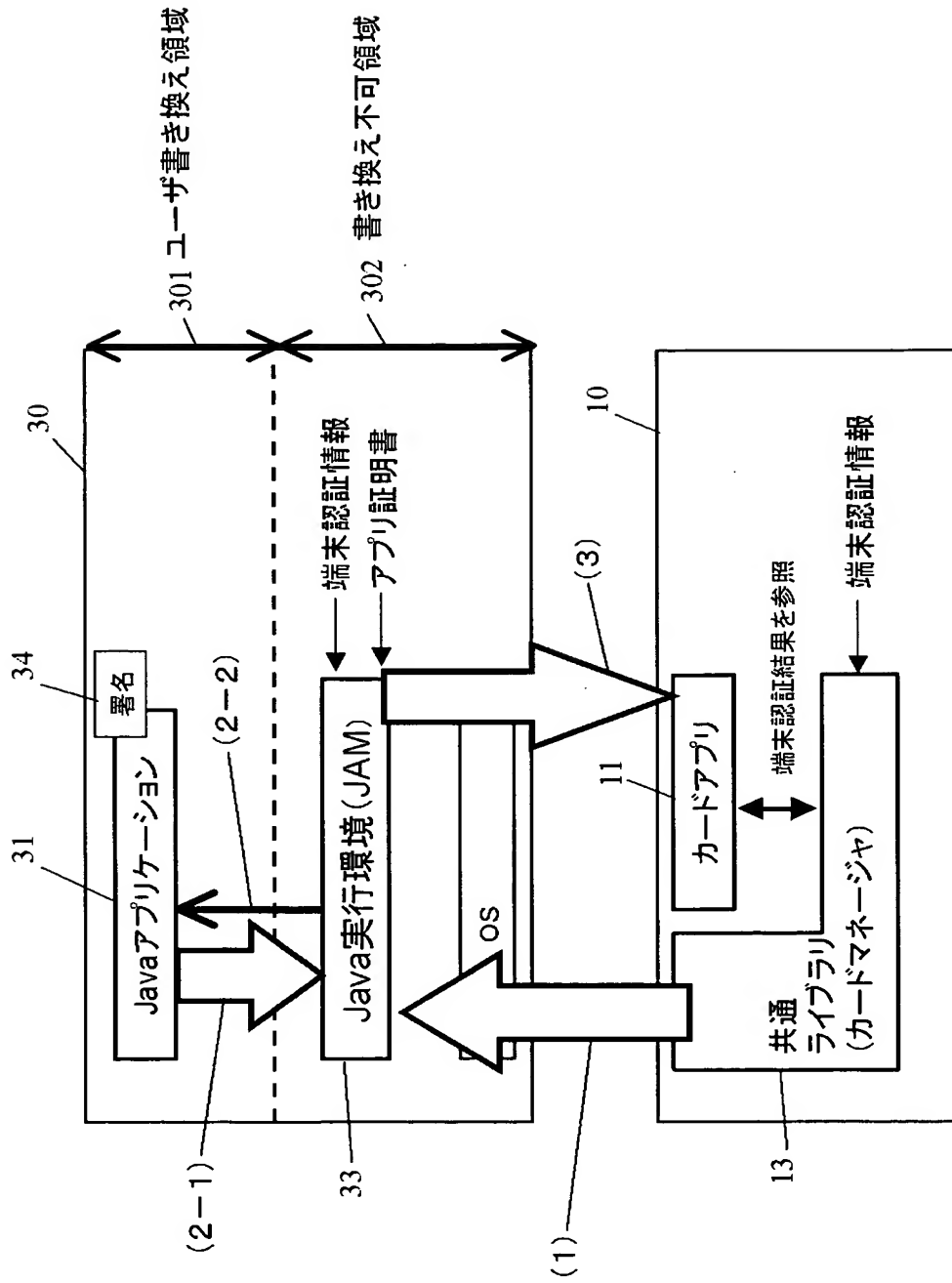
【図 3】



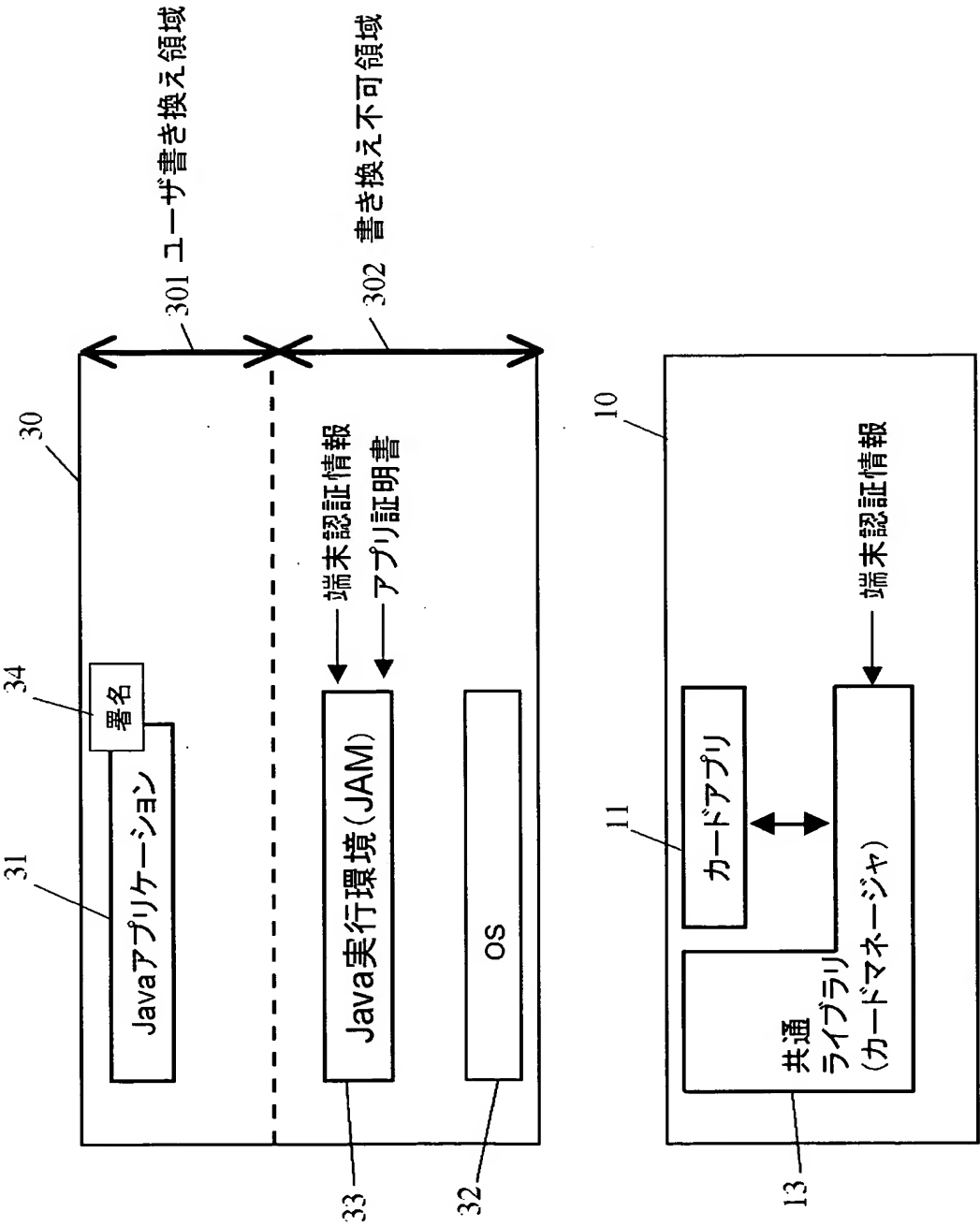
【図 4】



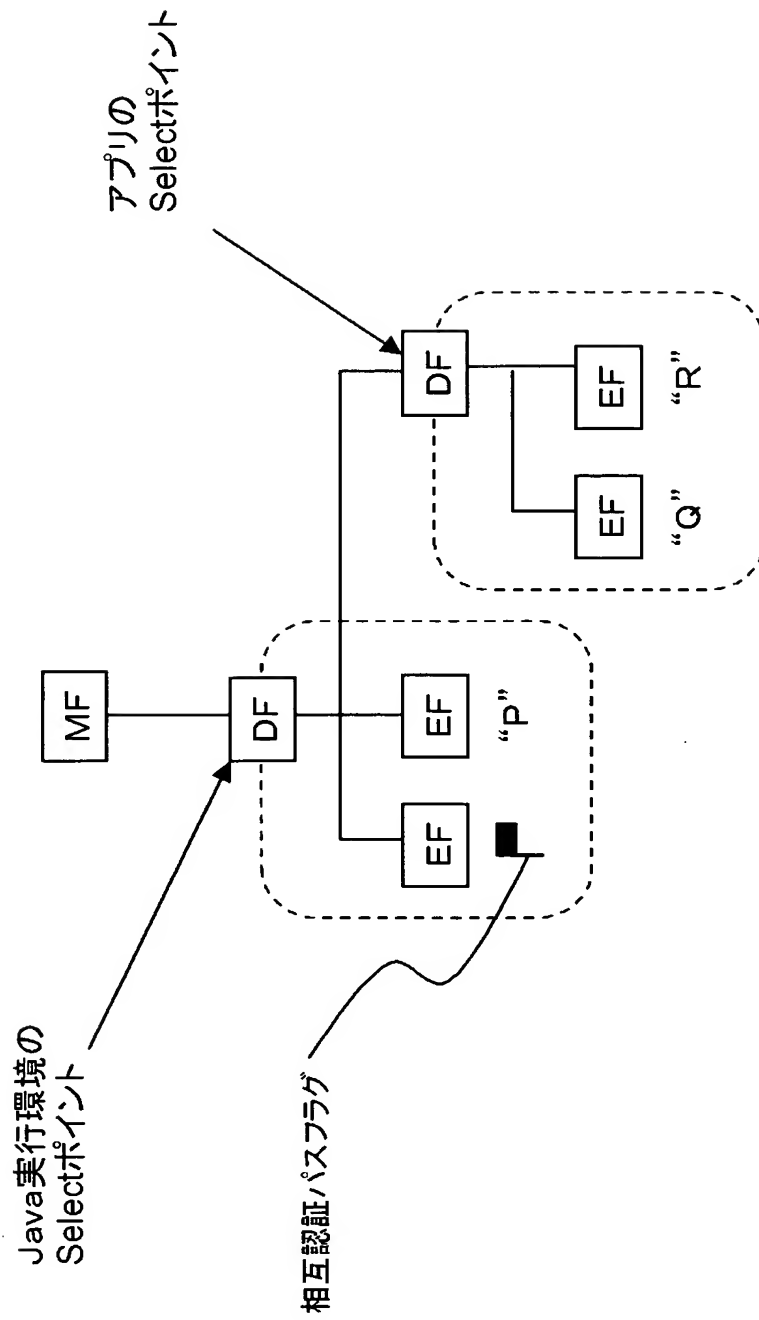
【図 5】



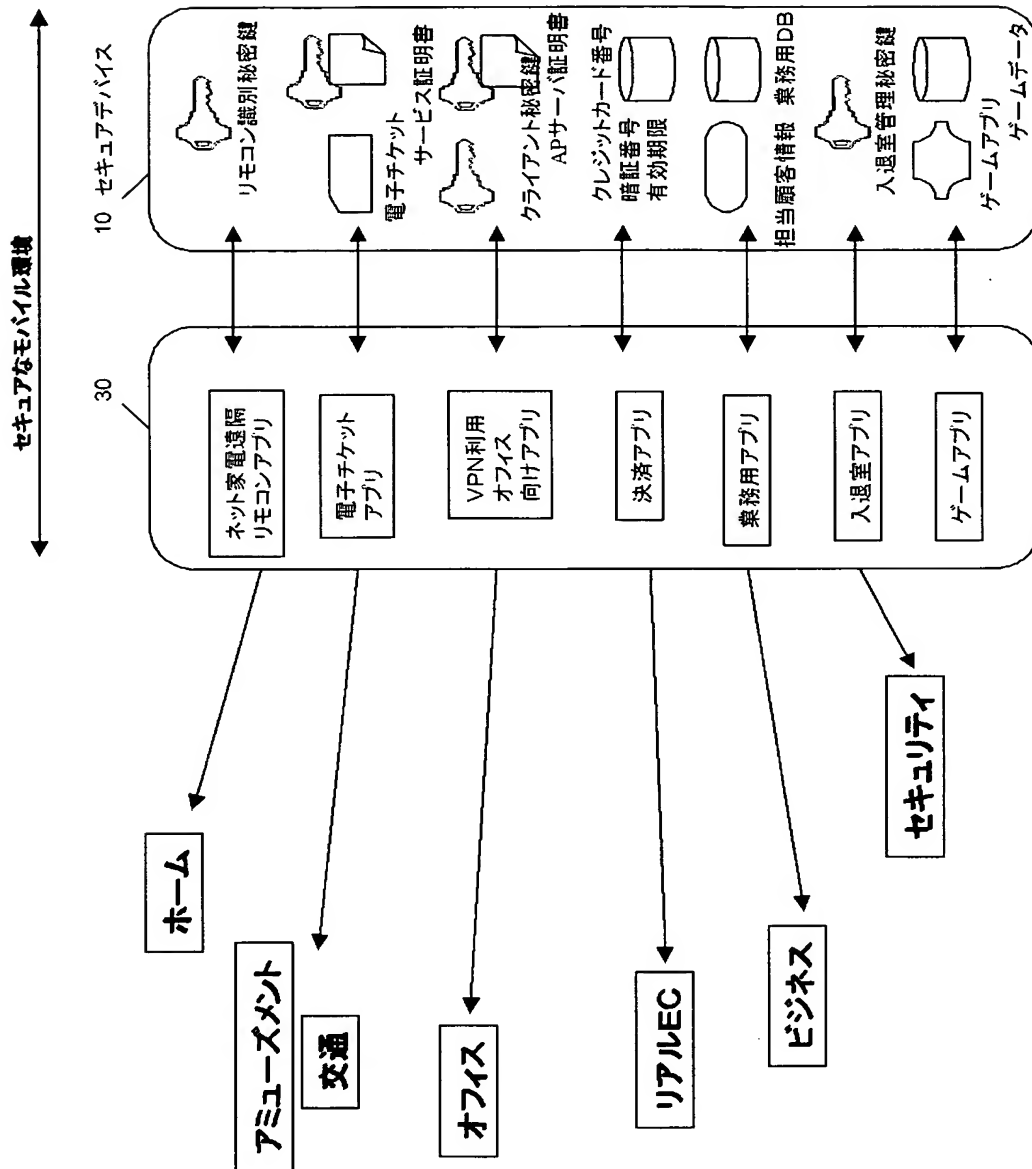
【図 6】



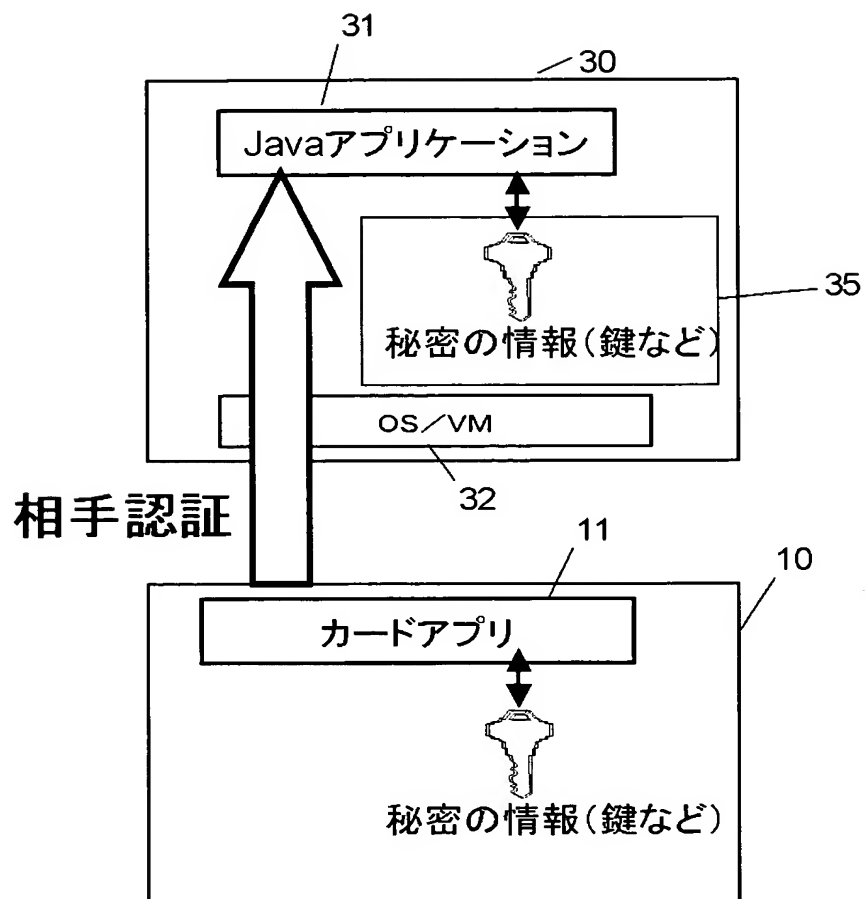
【図 7】



【図 8】



【図 9】



【書類名】 要約書

【要約】

【課題】 安全な情報秘匿領域を持たない端末上のアプリに対するセキュアデバイスの認証が可能なアプリケーション認証システムを提供する。

【解決手段】 安全な情報秘匿領域を持たない端末30に装着されたセキュアデバイス10が、端末に格納されたアプリ31を認証するアプリケーション認証システムにおいて、セキュアデバイス10が、端末の書き換え不可領域302に格納されたアプリ実行手段33を認証し、このアプリ実行手段が、セキュアデバイスへのアクセスを要求するアプリ31に対して行った処理に基づいて、アプリを認証するように構成している。セキュアデバイスと端末との相互認証、及び、端末内でのアプリの認証とを結び付けることで、安全な情報秘匿領域を持たない端末上で動作するアプリに対して、セキュアデバイスによる認証が可能になる。

【選択図】 図1

特願 2 0 0 3 - 0 5 3 3 6 2

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 8 2 1]

1. 変更年月日	1 9 9 0 年 8 月 2 8 日
[変更理由]	新規登録
住 所	大阪府門真市大字門真 1 0 0 6 番地
氏 名	松下電器産業株式会社